

**REMARKS**

Claims 1-34 are pending.

In the present Office Action, claims 1-34 stand rejected under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent No. 6,377,994 (hereinafter “Ault”). Applicant traverses these rejections and requests reconsideration and withdrawal of the above rejections.

In order for there to be anticipation, each and every element of the claimed invention must be present in a single prior reference. Applicant respectfully submits that each of the claims 1-34 recite elements which are not taught, suggested, or implied by Ault. In addition, Applicant notes that while the examiner cites various portions of Ault as disclosing certain features, it is in no way clear how the examiner believes the cited portions apply. Rather, the present Office Action merely repeats features of the pending claims and gives a citation which is purported to disclose such features. However, upon review, Applicant finds such citations bear little if any relevance to many of the features for which they are offered. The pertinence of each reference, if not apparent, must be clearly explained. 37 CFR 1.104(c)(2). If the examiner believes the cited disclosures to be pertinent, Applicant respectfully requests clarification.

In paragraph 3 of the present Office Action, it is suggested that Ault discloses all of the features of claims 1, 7, 10, 18, 26 and 32. For example, claim 1 recites a method which includes

“receiving a request for access to an object;

permitting access to said object in response to detecting said request is from a user, wherein a user community set (UCS) of said user is a superset of an object community set (OCS) of said object; and

permitting access to said object in response to detecting said request is from a process, wherein an application process community set (ACS) of said process is a superset of said OCS.” (emphasis added).

It is suggested that the above highlighted features are disclosed by Ault in the following excerpts:

"Clients 102 are processes that run either on separate workstations (not separately shown) or on a common workstation. Application servers 104 are processes that run on a host system 108. Host system 108 also includes one or more resources 110 accessed by application servers 104 on behalf of their clients 102, an operating system (OS) kernel 112, a host security server 114 for controlling access to resources 110, a host security database 116 containing access control information used by the host security server, and a "guest" security database 118 containing access control information used by "guest" application servers as described below. In the embodiment shown, it will be assumed that host system 108 is an IBM System/390 (S/390) processor, OS kernel 112 is the MVS OpenEdition kernel of the IBM OS/390 operating system, and that host security server 114 is the IBM Resource Access Control Facility (RACF), a component of OS/390. (IBM, System/390, S/390, MVS, OpenEdition, OS/390 and RACF are trademarks or registered trademarks of International Business Machines Corporation, the assignee.) The present invention is not limited to such a configuration, however.

...

Host security database 116 contains data defining the access rights of entities such as clients 102 and servers 104 seeking access to resources 110. As a prerequisite to determining the access rights of users seeking access to a resource, users are authenticated, i.e., established in some satisfactory manner (as by a password or other credentials) as being the entities they purport to be. In the disclosed system 100, users may be authenticated either to the host security server 114 (using a password or other credentials recognized by the host security server) or to DCE or some other guest system (using a password or other credentials recognized by the guest security server). Clients 102 that are not authenticated to the host security server 114 (even though they may be authenticated to a guest system such as DCE) are referred to herein as "unauthenticated" clients." (Ault, col. 3, lines 1-51).

However, as can be seen from the above, Ault merely discloses a host security database which defines access rights of clients and servers to resources. Ault further discloses that as a *prerequisite* to determining access rights to resource, users are authenticated (e.g., via logon password). However, there is no disclosure or suggestion concerning "a user community set (UCS) of said user is a superset of an object community set (OCS) of said

object" or "an application process community set (ACS) of said process is a superset of said OCS." Further, there is no disclosure of sets or set relations at all in Ault. Accordingly, the above features are not disclosed by Ault and the rejections of claims 1, 7, 10, 18, 26 and 32 of paragraph 3 should be withdrawn.

With respect to claims 4, 13, 21, and 29, it is suggested in paragraph 6 of the Office Action that Ault discloses these features at col. 3, lines 1-21 (reproduced above). However, upon inspection of the cited disclosure, there is no disclosure in the cited excerpt of the feature "wherein the initial owner of said object is the creator of said object." In fact, object ownership is not even mentioned in the whole of the Ault disclosure. Accordingly, the 35 U.S.C. § 102(e) rejection directed to these claims based on Ault is inappropriate.

Concerning the rejection of claims 5, 6, 14, 15, 22, 23, 30 and 31 in paragraphs 7-8 of the Office Action, each of these claims recite features directed to particular sets and set operations. However, Ault contains no disclosures concerning sets or set operations as recited. Accordingly, Applicant submits these rejections are properly withdrawn.

Finally, each of paragraphs 9 and 10 of the Office Action make rejections which suggest Ault discloses the recited community information base (CIB) with its particular recited features. The recited features include, for example, those of claim 8 "wherein said CIB includes a UCS for each user of said MCN, an ACS for application on said MCN, and an OCS for each object residing within said MCN" and claim 9 "wherein said CIB further includes a creator and a current owner for each object residing within said MCN." The cited portions of Ault are as follows:

"Host security database 116 contains data defining the access rights of entities such as clients 102 and servers 104 seeking access to resources 110. As a prerequisite to determining the access rights of users seeking access to a resource, users are authenticated, i.e., established in some satisfactory manner (as by a password or other credentials) as being the entities they purport to be. In the disclosed system 100, users may be authenticated either to the host security server 114 (using a password or other credentials recognized by the host security server)

or to DCE or some other guest system (using a password or other credentials recognized by the guest security server). Clients 102 that are not authenticated to the host security server 114 (even though they may be authenticated to a guest system such as DCE) are referred to herein as "unauthenticated" clients. Application servers 104 may access resources on behalf of such "unauthenticated" clients 102, but with additional restrictions as described below.

Each DCE user (or principal, to use the conventional DCE term) has what is known as a unique universal identifier (UUID) that specifies the user's identity in a DCE environment. A DCE client 102 authenticates itself to a DCE application server 104 by presenting satisfactory credentials to the server, which then accesses the guest security database 118 to verify the credentials and authenticate the DCE client. DCE credentials take the form of a privilege attribute certificate (PAC) specifying among other things the UUID of the client principal 102 and the groups of which the principal is a member. The manner in which PACs are formed under the DCE protocol is well known in the art and forms no part of the present invention." (Ault, col. 3, lines 41-67).

However, this excerpt of Ault merely discloses a host security database which defines access rights. Also disclosed are DCE credentials and the manner in which PACs are formed under DCE. There is nothing here which discloses the above recited features concerning a CIB and the recited sets.

In view of the above, Applicant submits the pending claims are patentably distinguishable from the cited art. Accordingly, withdrawal of the rejections is requested. Should the examiner disagree, a telephone interview is requested by the below signed representative at (512) 853-8866.

**CONCLUSION**

Applicants submit the application is in condition for allowance, and an early notice to that effect is requested.

If any extensions of time (under 37 C.F.R. § 1.136) are necessary to prevent the above referenced application(s) from becoming abandoned, Applicant(s) hereby petition for such extensions. If any fees are due, the Commissioner is authorized to charge said fees to Meyertons, Hood, Kivlin, Kowert, & Goetzel, P.C. Deposit Account No. 501505/5181-75800/RDR.

Also enclosed herewith are the following items:

Return Receipt Postcard

Respectfully submitted,

  
Rory D. Rankin  
Reg. No. 47,884  
ATTORNEY FOR APPLICANT(S)

Meyertons, Hood, Kivlin,  
Kowert, & Goetzel, P.C.  
P.O. Box 398  
Austin, TX 78767-0398  
Phone: (512) 853-8800

Date: April 12, 2005